REMARKS

Claims 21-31 remain in the application.

The Rejections:

In the Final Office Action dated August 10, 2006, the Examiner rejected Claims 21-31 under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The Examiner stated that Claims 21 and 31 recite a non-functional descriptive invention in that the claims state steps of instructions to be initiated within a building, but fails to include any computer readable medium or computer hardware to process or store the method of initiating a procedure within a building.

The Examiner rejected Claims 21-31 under 35 U.S.C. 103(a) as being unpatentable over Kanevsky, et al. (US 6,421,453) and further in view of An, et al. (US 6,715,073).

As per Claim 21, the Examiner stated that Kanevsky discloses a method of initiating a procedure within a building comprising the steps of:

defining at least one initiating event for the procedure; [col. 1, lines 49-52 and col. 16, lines 13-40]

defining at least one requirement for the procedure; [col. 1, lines 52-56; the requirement for the procedure (to access the facility) is a gesture pin or password]

defining at least one person to be authorized to perform the procedure; [col. 1, lines 57-63]

detecting the occurrence of the at least one initiating event; [col. 1, lines 65-67 and col. 9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col. 1, lines 16-22)]

generating a virtual key for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event; [col. 15, lines 29-37 and col. 17, lines 23-37]

transmitting virtual key to the at least one person; [col. 18, lines 30-32]

detecting use of the virtual key; [col. 17, lines 46-61]

checking the validity of the virtual key; and [col. 5, lines 39-43 and col. 15, lines 40-45]

initiating said procedure within the building if the validity check is positive. [col. 4, lines 61-66 and col. 9, lines 10-28]

The Examiner further stated that virtual key can obviously be Kanevsky's gesture pin or password that is used to verify the person or user to gain access to the building or facilities (col. 5, lines 40-43 and col. 8, lines 23-40). The Examiner commented, however, that Kanevsky does not specifically disclose the virtual key is a password. The Examiner stated that An teaches digital keys are replacing user identification password pairs, digital signatures are replacing physical signatures to guarantee the identity of the sender, organizations controls access for customers or users by registering user identification and passwords, and the password is a virtual key that authenticates a user (col. 1, lines 43-48 and col. 2, lines 4-10). According to the Examiner, it would have been obvious for a person of ordinary skills in the art at the time of the invention that a virtual key as taught by An can be the gesture pin or password as taught by Kanevsky because the virtual key (or gesture password) authenticates the user to allow access to something (i.e. building or facilities).

As per Claim 22, the Examiner stated that An (col. 1, lines 64- col. 2, line 1) discusses a step of assigning an encrypted code to the virtual key.

As per Claim 23, the Examiner stated that An (col. 2, lines 5-12) discusses the steps of adding a signature to the virtual key and identifying a recipient of the transmitted virtual key by the signature.

As per Claim 24, the Examiner stated that Kanevsky (col. 1, lines 49-55) discusses defining different procedures for different initiating events.

As per Claim 25, the Examiner stated that Kanevsky (col. 13, lines 59-62 and col. 29-53) discusses defining different requirements for different procedures.

As per Claim 26, the Examiner stated that Kanevsky (col. 9, lines 25-27) and An (col. 1, lines 64- col. 2, line 12) discuss transmitting different virtual keys to said person for different initiating events.

As per Claim 27, the Examiner stated that Kanevsky (col. 17, lines 20-30) discusses storing said virtual key partially or completely.

As per Claim 28, the Examiner stated that Kanevsky (col. 17, lines 20-30) discusses the steps of identifying the at least one person with biometrics characteristics.

As per Claim 29, the Examiner stated that Kanevsky discloses classification involves the differentiation of multiple individuals attempting to interact with the system and a purpose of identify the individuals from their respective commands (col. 1, lines 49-58), it is desirable to implement an extension of the identification task where the individuals attempting to interface with the computer are ranked so that a higher ranking individual (i.e. supervisor) is allowed access over a lower ranked individual (i.e. data entry person) (col. 1, line 65- col. 2, line 1), and the concept of biometrics and its application to security tasks where such task could include providing access control in a natural computing environment as well as access control to a service, facility, or goods (col. 9, lines 23-28). According to the Examiner, it is obvious that initiating a variety of procedures such as for an elevator in a building, medical assistance, building cleaning procedure or guest reception is Kanevsky's security tasks that include classification and identification of particular users or procedures.

As per Claim 30, the Examiner stated that (Kanevsky?) (col. 31, lines 63-64) discusses the step of transmitting the virtual key using wireless devices.

As per Claim 31, the Examiner stated that:

Method of initiating a procedure within a building comprising the steps of:

defining at least one initiating event for the procedure; [col. 1, lines 49-52 and col. 16, lines 13-40]

defining at least one of a security requirement and an availability requirement for the procedure; [col. 1, lines 52-56; the security requirement for the procedure (to access the facility) is a gesture pin or password or a question or biometrics for the particular procedure (col. 13, lines 17-62 and col. 15, lines 30-55)]

defining at least one person to be authorized to perform the procedure; [col. 1, lines 57-63]

detecting the occurrence of the at least one initiating event; [col. 1, lines 65-67 and col. 9, lines 1-3; detecting the occurrence is when the person comes to the interacting system or interface area (col. 1, lines 16-22)]

generating a virtual key for the at least one based on the at least one requirement detecting the occurrence of the at least one initiating event; [col. 15, lines 29-37 and col. 17, lines 23-37]

transmitting virtual key to the at least one person; [col. 17, lines 38-45 and col. 18, lines 30-32]

detecting use of the virtual key; [col. 17, lines 46-61]

checking the validity of the virtual key; and [col. 5, lines 39-43 and col. 15, lines 40-45]

initiating said procedure within the building if the validity check is positive. [col. 4, lines 61-66 and col. 9, lines 10-28]

The Examiner stated that the virtual key can obviously be Kanevsky's gesture pin or password that is used to verify the person or user to gain access to the building or facilities (col. 5, lines 40-43 and col. 8, lines 23-40). The Examiner commented that Kanevsky does not specifically disclose the virtual key is a password. The Examiner further stated that An teaches digital keys are replacing user identification password pairs and digital signatures are replacing physical signatures to guarantee the identity of the sender, organizations controls access for customers or users by registering user identification and passwords, that the password is a virtual key that authenticates a user (col. 1, lines 43-48 and col. 2, lines 4-10), and it would have been obvious for a person of ordinary skills in the art at the time of the invention that a virtual key as taught by An can be the gesture pin or password as taught by Kanevsky because the virtual key (or gesture password) authenticates the user to allow access to something (i.e. building or facilities).

Applicants' Response:

Applicants continue to disagree with the Examiner's rejection under 35 U.S.C. 101. However, in order to overcome this rejection, Applicants amended independent Claims 21 and 31 to include the step "j. performing said steps a. through i. in an access control computer system associated with the building." Support for this amendment is found on Page 6 at Lines 7-8 of the specification.

The method according to the present invention generates a virtual key in response to the detection of the occurrence of a certain event. (Page 2, Lines 22-23) The person to whom the key is communicated is made to depend on the type of event. (Page 3, Lines 1-2) The event can be an emergency call, an order, a request such as for a cleaning service, an invitation, or a periodically recurring event such as, for example, monitoring a condition, or a service. (Page 3, Lines 23-25) The type of event determines what requirements are specified for the key such as security and availability. (Page 3, Lines 26 to Page 4, Line 3)

It is through the event that the person to be authorized is defined. (Page 4, Line 5) The person is defined in a processing step "Specify Person to be Authorized" **13**. (Page 4, Lines 8-9) As shown in the drawing of the flowchart for the method according to the present invention, the event occurs at the starting point **11** which is before the step **13** of specifying the person to be authorized.

Thus, Claims 21-31 define a method in which the virtual key is generated only when the initiating event occurs and is detected. Only then is the virtual key generated and transmitted to an authorized person. Therefore, Claims 21-31 define a method whereby an authorized person can only access a building if the initiating event has indeed occurred. Examples, of such initiating events are set forth on page 3 of Applicants' specification at lines 23-25.

Applicants also amended step e. of Claims 21 and 31 to recite "generating a virtual key for the at least one person based on the at least one requirement upon detecting the occurrence of the at least one initiating event and prior to the at least one person arriving at the building". Applicants believe that this amendment distinguishes the claimed method from the Kanevsky patent that shows a method and a system for user recognition employing behavioral passwords to access a computer, a service, or a facility. According to the Examiner, the initiating event is the presence of a computer user and the "gesture pin" is the virtual key that is generated and stored before the "initiating event". This is the opposite order of Applicants' steps d. and e.

The Examiner made of record but did not discuss references to Saito et al. (US6980672), DeLaHuerga (US6779024), Talati et al. (US5903878), Brooks (US6898299) and Sehr (US6999936). Applicants reviewed these references and found them to be no more pertinent than the prior art relied upon by the Examiner in the rejections.

In view of the amendments to the claims and the above arguments, Applicants believe that the claims of record now define patentable subject matter over the art of record. Accordingly, an early Notice of Allowance is respectfully requested.